REMOTE ACCESS	
Policy Number: IT-040	**Responsible Department: Information Technology**
Effective Date: 12/01/2016	**Last Revision Date: 12/19/2016**

PURPOSE:

To state the requirements for remote access to computing resources hosted at CWI using Virtual Private Network (VPN) technology.

SCOPE:

Applies to all CWI Users.

DEFINITIONS:

Information Technology (IT) Resources: An array of products and services that collect, transform, transmit, display, present, and otherwise make data into usable, meaningful and accessible information. IT Resources include but are not limited to: desktop computers, laptops, and tablet PC's; handheld devices including but not limited to, cell phones; e-mail, voicemail, servers, central computers, and networks; cloud storage systems; network access systems including wireless systems; portable hard drives and databases; computer software; printers and FAX machines and lines; campus, classroom and office audio and visual display devices and switching, camcorders, televisions, physical media; telephone equipment and switches including local and long-distance services; satellite equipment and any other current or future IT resource adopted by CWI as new technologies are developed.

Remote Access: Access to IT Resources from an electronic or other device not directly connected to the CWI wired or wireless networks, but not including accesses to such IT Resources where Remote Access is considered a primary function and normative use. For example, use of a Web browser to remotely access a CWI Web page is not covered by this policy.

Remote User: One who uses an electronic or other device for Remote Access.

User: Anyone who uses CWI's information technology resources, even if they have no responsibility for managing the resources. This includes students, faculty, staff, contractors, consultants, and temporary employees.

Virtual Private Network (VPN): a secured private network connection built on top of a public network. A VPN provides a secure encrypted connection or tunnel over the Internet between a CWI individual computer and a private network. VPN allows members of CWI to securely access CWI network resources as if they were on campus.

POLICY

Remote Access to CWI's IT Resources must be accomplished in a manner that furthers CWI's mission while preventing unauthorized use of those resources. This policy is designed to ensure that CWI's IT Resources are used for the purposes for which they are intended. Accordingly, CWI prohibits illegal or unauthorized Remote Access to CWI's IT Resources. Only authorized CWI employees may utilize CWI's VPN for Remote Access.

GUIDELINES

In order to connect to the VPN it is necessary for Remote Users to install the approved Cisco Anyconnect Software on a laptop provided by CWI (software URL will be provided). Remote Users will need a connection to the Internet from their off-campus location. CWI does not provide Remote Users with an Internet connection, their Internet Service Provider does.

- It is the responsibility of all employees with Remote Access privileges to ensure that unauthorized users are not allowed access to internal CWI networks and associated content.
- Remote Access is subject to all applicable CWI policies.
- All employees, while using CWI's VPN technology for Remote Access, are a de facto extension of the CWI network, and as such are subject to the CWI Internet Usage Policy.
- All computers or electronic devices connected to CWI's internal network via the VPN or any other technology must use a properly configured up-to-date operating system and anti-virus software.
- Redistribution of the CWI VPN Cisco client or associated installation information is prohibited.
- All employees using CWI's VPN shall only connect to or have access to machines and resources that they have permission and rights to use.
- Support will only be provided for VPN clients approved by CWI's Information Technology Services.
- All Remote Users must use the centrally provided VPN client software.
- All systems used for Remote Access must have an enabled firewall.
- All employees must recognize that the use of the VPN system does not guarantee that all transmissions between the remote PC and the CWI network are secure. It is the Remote User's responsibility to configure their applications to use the VPN if they desire their transmissions to be secure.

ENFORCEMENT

CWI's Chief Information Officer is responsible for enforcement of this policy.

VIOLATION OF POLICY

Any violation of this policy may result in corrective action up to and including termination of employment and/or suspension or expulsion in the event of a student. Additionally, Users who violate this policy may be subject to loss of software privileges, civil action and criminal prosecution.